PORTABLE DATA STORAGE DEVICE WITH LAYERED MEMORY ARCHITECTURE

Field of Invention

This invention relates to a portable data storage device which is capable of storing and easily transporting large amounts of data and in which access to the data can be secured by a polynominal key generated by pseudo random generated parameters and wherein the device can act as a host or a client in respect of access to the data thereby providing protection not only for the data held within the device but also to the computer to which the device is attached and wherein data is stored in layered memory architecture providing a secure primary and secondary partition structure.

Summary of Invention

This invention provides a data storage disk disposed with a communications interface which uses encryption technology and host/client switchable technology to create a novel architecture and communications protocol to ensure data stored in the disk is secured by means of pseudo random generated parameters and at the same time the architecture provides the user with layer protection which employs a self initiated host/client switchable controller which secures access not only to the data but also access to any host computer to which the disk is attached.

Data stored within the disk is secured by means of memory partition architecture and data protection protocol and procedure such that data within the memory storage is layered and encrypted by reference to a pseudo random generated key. As a consequence of such security it would be impossible for any one to access the

data without the primary key input.

The data storage disk is disposed with:

1. A communications interface;
2. A microcontroller with built in switchable input;
3. a primary and secondary memory storage means;
4. A data processing unit;
5. Data and decision means;
6. Secure key processing unit;
7. An access control decision unit;
8. An encrypted smart key storage unit.

The communications interface which may be a USB type interface or other communications interface permits users to access the data stored in the memory means of the device. The communications interface enables a user to reversibly access the data in the storage disk.

The microcontroller is disposed with a switchable input interconnected to a data and decision means for primary and secondary layer memory access. The microcontroller and data and decision means are responsible for interfacing between a host computer and the memory storage means and as such provide a gateway for data storage and retrieval and the processing in and from the flash memory means for authorised users.

The primary and secondary storage means are used to store data to permit selective access to users in accordance with the authorisation granted to the user and access to such data is secured by reference to a secure encrypted key.

The switchable input can be initiated by a host computer to which the device is attached wherein the device acts as a client or the input can be initiated by the microcontroller itself wherein the device acts as a host. Key input can be made from the host computer or directly from the device itself. Such key input can then be analysed by the data and decision means for access to primary and secondary layer memory.

The secure key processing unit is reversibly interconnected with an encrypted smart key storage unit and is further connected to the access control decision unit. The access control decision unit is connected to the data processing unit.

The data processing unit is reversibly interconnected to a primary and secondary flash memory means and is accessed by the and interconnected with the communications interface. The data processing unit permits two way access to the layered memory means.

Access to the data which is stored in the device by reference to an encrypted polynominal key which is generated by reference to a user key input in combination with a factory preset code. To access the data held in the memory means an enrolled user is obliged to input his/her key directly to the device or to a host computer to which the device is connected. By permitting such switchable input access control it enables the user of the device to permit authorised third parties to access the data held in the device via an approved computer host device.

The input key is converted to a pseudo random generated key by means of

encryption technology. This encrypted user input key is stored in the memory means. To this encryption key the secure key processing unit adds a factory preset code in a polynominal appending process to produce a secure key. Thus the secure polynominal key is based on a user input key and a factory preset code. This secure encrypted polynominal key is stored in the memory means.

Access to the data requires the user to input the appropriate user key input either through the device or through an approved host computer to which the device is attached. Authentication of the input key permits the user to proceed to encryption key generation procedure and primary and secondary memory access.

Enrollment of users requires users to input a key of their own choice either directly to the device or via the host computer to which the device is attached. The user key is encrypted by reference to pseudo random generated parameters and stored in the memory means. This encrypted key is
then combined with a factory preset code to form a secure polynominal key. Such key is pointed and is accessible by a key known as an encryption pointer. User access can be selectively restricted either the primary or secondary memory layer or to both layers.

To access data the user will input his/her input key. The data and decision means for access to the primary and/or secondary layer memory authenticates the user input. An encryption pointer is then prepared by to retrieve the encryption key from the secure partition memory. The encryption key is then combined with the factory preset key to generate a secure polynominal key. This polynominal key is then decrypted by the secure key processing unit. The access control decision unit

then grants access to the data which is processed by the data processing unit.

By partitioning the memory means it is possible to selectively restrict access that users may have to the data held in storage. This is achieved by means of layered encryption architecture. The highest level of authorisation would permit the user to all the data stored in the different memory partitions while lower level of authorisation would restrict access to data held in one or other partition layer. It is thus possible to enable a user to permit third parties to access some or all of the data held in the device through selective enrollment procedure. Such third party users would be able to access the data through an authorised host computer by inputting their user key.

Brief Description of the Drawings

The invention will now be described by reference to the drawings.

Figure 1 is a block diagram of the system components.

Figure 2 is a flowchart of the key encryption scheme for access to the primary and secondary memory means.

Detailed Description of the Preferred Embodiments

Figure 1 is a block diagram of the system components. The device is disposed with a communications interface (10) which links the device to a host computer and which is in two way communication with a data processing unit (9). The data processing unit is in communication with an access control decision unit (6) and the primary data storage unit (7) and the secondary data storage unit (8). The

access control decision unit is in communication with and receives input from the secure key processing unit (4).

The secure key processing unit is in two way communication with the encrypted smart key storage unit (5) and is also in communication with and receives input from the data and decision means (3) for access to the primary and/or secondary layer memory means and the communications interface.

The data and decision means (3) is in communication with and receives key input from the host computer (11) and/or key input from the device itself (12). The key input is in communication with a micro controller (1) which is in communication with a switchable input (2).

Figure 2 shows the flow chart of key encryption scheme to access the memory means. At the start of the process the user inputs his/her key input (20). This user key input is then authenticated (21) by the data and decision means (3). The user key input is then evaluated to determine whether the user is entitled to primary and/or secondary level memory access (22). This process is also carried out by the data and decision means (3).

Once the use key input has been authenticated and its access class determined an encryption pointer key is prepared (23). The encryption key in respect of enrolled users is retrieved from the secure memory means (24) for primary level access and (25) for secondary level access by preparing a primary or secondary encryption pointer key.

A secure key is then generated (26) by the secure key processing unit (4) by a

polynominal appending process in which the factory encrypted key (27), stored in the encrypted smart key storage unit (5) and the encrypted user key input are combined.

This secure key is then decrypted (28) by the data processing unit (9) to permit the user access to the primary (29) and/or the secondary (30) level memory means. The data can then be accessed via the communications interface (10) linked to a host computer (31).